UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/464,347	12/15/1999	JEFFREY A. MORGAN	10179US01	7422

7590 11/21/2003

ERIC D LEVINSON
IMATION CORP
LEGAL AFFAIRS
PO BOX 64898
ST PAUL, MN 551640898

EXAMINER	
TRIEU, LAURENT L	

ART UNIT	PAPER NUMBER
2132	4

DATE MAILED: 11/21/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/464,347	MORGAN ET AL.	
	Examiner	Art Unit	
	Laurent Trieu	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 December 1999* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-67* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-67* is/are rejected.

7)☒ Claim(s) *25* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-67 are pending.

2. Claim 25 objected to because of the following informalities: "Biometric" is misspelled. Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1 and 2 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. Claim 1 recites the limitation "the device-specific security information" in lines 3 and 6. This is not mentioned previously thus there is insufficient antecedent basis for this limitation in the claim.

6. Claim 2 recites the limitation "the storage disk". This is also not mentioned previously thus there is insufficient antecedent basis for this limitation in the claim.

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-6, 8, 12-21, 26-33, 39-43, 45-49, 51-54, 56-61 and 63-67 are rejected under 35 U.S.C. 102(b) as being anticipated by Narasimhalu et al, US Patent # 5,412,718, hereafter referred as Narasimhalu.

9. Claims 1, 12& 13 are rejected as follows:

10. Claim 1 states:

> sensing whether a storage device has security information stored thereon;

Narasimhalu discloses "nonuniformities 41-47 are detected with a nonuniformities detection program (NDP)." - Column 4, lines 35-36

> operating the computer in a full-access mode when the storage device has the device-specific security information;

Narasimhalu discloses, "With the decryption key from 220, the present invention enables the information consumer to decrypt the encrypted information (EDI)" – Column 7, lines 26-29 and

> operating the computer in a restricted-access mode when the storage device does not have the device-specific security information.

Narasimhalu discloses "a key for encrypting the information on the storage medium." (Column 2, lines 25-27)

11. Claim 12 states:

> The method of claim 1 wherein sensing the storage device is performed when a status change is detected for the storage device.

12. Claim 13 states:

> The method of claim 12, wherein the status change indicates the insertion of the storage device into the computer.

According to claim 1, "sensing whether a storage device has security information stored thereon" is read to include claims 12 & 13. Prior to "sensing for security information", one first has to detect a status change in the storage device to recognize whether or not a storage apparatus is inserted, then sense for the security information.

13. Claim 2 states:

> The method of claim 1, wherein operating the computer in a full-access mode includes the following:
> encrypting digital data to be written to the storage disk; and

Narasimhalu discloses, "a key for encrypting the information on the storage medium." (Column 2, lines 25-27)

> decrypting digital data read from the storage device.

Narasimhalu discloses, "Decryption of the information is accomplished by generating a key...." (Column 2, lines 39-41)

14. Claims 3, 4 and 14 are rejected as follows:

Claim 3 states:

The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from format information for the storage device.

Claim 4 states:

The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information etched on the storage device during manufacturing.

Claim 14 states:

The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from security information written to the storage device during low-level formatting.

Narasimhalu discloses, "Copy protection is achieved by generating a signature from a given storage medium. The signature is derived from an arbitrarily selected list of nonuniformities, uniformities and their attributes." - Column 2, lines 18-22)

"Selected list of nonuniformities, uniformities and their attributes" is read to include "format information", "information etched on the storage device during manufacturing" and "security information written to the storage device during low-level formatting."

15. Claim 5 states:

The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information specific to a removable media drive used for accessing the storage device.

Claim 58 states:

The computer of claim 51, wherein the storage device is a removable storage medium.

Claim 59 states:

The computer of claim 51, wherein the storage device is a data storage diskette.

Claim 60 states:

The computer of claim 51, wherein the storage device has a disk-shaped storage medium.

Narasimhalu discloses, "By storage medium, the present invention refers to all types of non-volatile storage medium. Examples of such media include floppy disks, hard disks, optical disks and other non-volatile semiconductor storage devices." – Column 1, lines 25- 29.

16. Claim 6 states:

The method of claim 5, wherein the drive-specific information includes a drive serial number.

Narasimhalu discloses, "One such method uses as key the hardware serial number or identification number." (Column 1, lines 37-38)

17. Claim 8 states:

The method of claim 1 wherein operating the computer in a restricted-access mode includes operating the storage device in a read-only mode.

Narasimhalu discloses, "There are two possibilities for the incorrect signature: (1) a read/write peripheral fails to transfer the nonuniformities from the distribution medium to a copied medium, or (2) the storage medium is a copied or unauthorized medium. Both outcomes are detected by the SVP in step 175. It follows that an evade program is invoked in step 180 to halt the program

altogether." (Column 6, line 67 – Column 7, line 6) "To halt the program

altogether" is read as "operating the storage device in a read-only mode."

18. Claim 15 states:

The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from a unique identifier stored within an electronic circuit embedded within the storage device.

Narasimhalu discloses, "the use of an unique identification stored in read only memory of a personal computer." – Column 1, lines 60-62. "Read only memory" (ROM) is read to comprise "an electronic circuit."

19. Claim 16 states:

A method for accessing a storage device comprising:
detecting a storage device within the storage drive;
sensing whether a storage device has security information stored thereon;

Narasimhalu discloses "nonuniformities 41-47 are detected with a nonuniformities detection program (NDP)." - Column 4, lines 35-36. "Sensing a storage device" is read to comprise "detecting a storage device within the storage drive."

and performing at least the following when the storage device has the device specific security information:

encrypting digital data using the security information during a write access to write the digital data to the storage device; and

Narasimhalu discloses, "a key for encrypting the information on the storage medium." - Column 2, lines 25-27]

decrypting digital data using the security information during a read access to read the digital data from the storage device.

Narasimhalu discloses, "Decryption of the information is accomplished by generating a key...." - Column 2, lines 39-41.]

20. Claim 17 states:

> The method of claim 16, wherein encrypting the digital data includes generating a cryptographic key as a function of format characteristics of an underlying storage medium of the storage device.

Narasimhalu discloses, "The signature is derived from an arbitrarily selected list of nonuniformities, uniformities and their attributes." Column 2, lines 20-22. Furthermore, "This signature is used to derive a key for encrypting the information on the storage medium." – Column 2, lines 25-27.

21. Claim 18 states:

> The method of claim 16, wherein encrypting the digital data includes generating a cryptographic key as a function of a unique identifier stored within an electronic circuit embedded within the storage device.

Narasimhalu discloses, "the use of an unique identification stored in read only memory of a personal computer." – Column 1, lines 60-62. "Read only memory" (ROM) is read to comprise "an electronic circuit."

22. Claims 19, 39-41 are rejected as follows:

Claim 19 states:

> The method of claim 16 and further including preventing data from being written to the storage device during a write access when the storage device does not store the device-specific security information.

Claim 39 states:

> A method for operating a storage drive comprising:
> configuring the storage drive to operate in a read-only mode upon power-up;
> determining whether the storage device has device-specific security information written thereon; and
> configuring the storage drive to operate in a read/write mode when the storage device within the storage drive has device-specific security

information written thereon.

Claim 40 states:

The method of claim 39 and further including configuring the storage drive to operate in a read-only mode when the storage device within the storage drive does not have device-specific security information written thereon.

Claim 41 states:

The method of claim 39 and further including preventing all read and write access to the storage device when the storage device within the storage drive does not have device-specific security information written thereon.

Narasimhalu discloses, "There are two possibilities for the incorrect signature: (1) a read/write peripheral fails to transfer the nonuniformities from the distribution medium to a copied medium, or (2) the storage medium is a copied or unauthorized medium. Both outcomes are detected by the SVP in step 175. It follows that an evade program is invoked in step 180 to halt the program altogether." (Column 6, line 67 – Column 7, line 6) "To halt the program altogether" is read "to prevent data from being written to the storage device..." "Otherwise, the positive matching of the device Ids in step 200 activates the decryption key generating program (DKGP) in step 220." This is read to enable access / security mode.

23. Claim 20 states:

A method for accessing a storage device comprising:
detecting a storage device within the storage drive;
sensing whether a storage device has device-specific security information stored thereon;
encrypting digital data using the device-specific security information when the storage device has the device-specific security information;
and writing the encrypted digital data to the storage device.

Claim 53 states:

The computer of claim 51, wherein the drive includes drive-specific information stored in a non-volatile memory, and further wherein the storage manager generates a cryptographic key as a function of the

drive-specific information and decrypts data stored on the storage device using the generated key.

Claim 54 states:

The computer of claim 51, wherein the storage device includes a serial number physically etched onto the storage device during manufacturing, and further wherein the storage manager generates a cryptographic key as a function of the serial number and decrypts data stored on the storage device using the generated key.

Claim 56 states:

The computer of claim 51, wherein the format information of the storage device includes a primary defect list.

Claim 57 states:

The computer of claim 51, wherein the format information of the storage device includes one or more logical block addresses.

Narasimhalu discloses, "The signature is derived from an arbitrarily selected list of nonuniformities, uniformities and their attributes." (Col. 2, lines 20-22). This reads as "device-specific security information", "serial number". Furthermore, "This signature is used to derive a key for encrypting the information on the storage medium."

Also, "...nonuniformities 41-47 are detected with a nonuniformities detection program (NDP)." - Column 4, lines 35-36. "Sensing a storage device" is read to comprise "detecting a storage device within the storage drive." It also discloses, "a key for encrypting the information on the storage medium." (Col. 2, lines 25-27) Narasimhalu further discloses, "Decryption of the information is accomplished by generating a key...." (Column 2, lines 39-41)

24. Claims 21 & 26 are rejected –

Claim 21 states:

The method of claim 20, wherein encrypting digital data using the device-specific security information generating a cryptographic key as a function of low-level format information for the storage device.

Claim 26 states:

> The method of claim 21, wherein the format information includes a primary defect list.

Narasimhalu discloses, "The signature is derived from an arbitrarily selected list of nonuniformities, uniformities and their attributes." Column 2, lines 20-22. Furthermore, "This signature is used to derive a key for encrypting the information on the storage medium." (Column 2, lines 25-27)

"List of nonuniformities, uniformities and their attributes" is read to comprise "low-level format information" and "defect list"

25. Claim 27 states:

> The method of claim 21, wherein the format information includes one or more logical block addresses.
>
> The computer of claim 51, wherein the format information of the storage device includes one or more logical block addresses.

Narasimhalu discloses, "... this invention refers to the characteristics of bits on a storage medium which includes but not restricted to the track number, sector number, length, readability and writability." This is read to comprise "logical block addresses." (Column 4, lines 50-54)

26. Claims 28 –29 are rejected.

Claim 28 states:

> The method of claim 21, wherein generating the key includes computing an arithmetic sum of the format information.

Claim 29 states:

> The method of claim 21, wherein generating the key includes evaluating a polynomial using the format information as data for the polynomial.

Narasimhalu discloses, "It should be understood by one skilled in the art that the function utilized by the SGP could be a mathematical or some other pre-determined manipulation.

"Mathematical manipulation" is read to include "computing an arithmetic sum of the format information" and "evaluating a polynomial using the format information as data for the polynomial"

27. Claims 30 & 31 are rejected.

Claim 30 states:

> The method of claim 20, wherein writing the encrypted digital data includes writing the encrypted digital data to a removable storage medium.

Claim 31 states:

> The method of claim 30, wherein writing the encrypted digital data includes writing the encrypted digital data to a data storage diskette.

Narasimhalu discloses, "By storage medium, the present invention refers to all types of non-volatile storage medium. Examples of such media include floppy disks, hard disks, optical disks and other non-volatile semiconductor storage devices." – Column 1, lines 25- 29.

"Floppy disks" is read to include "removable storage medium" and "data storage diskette."

28. Claim 32 states:

A method for securely accessing a storage device within a storage drive comprising:
retrieving drive-specific information from the storage drive;

Narasimhalu discloses "nonuniformities 41-47 are detected with a nonuniformities detection program (NDP)." - Column 4, lines 35-36. "Sensing a storage device" is read to comprise "retrieving drive-specific information from the storage drive."

generating a cryptographic key as a function of the drive-specific information;

Narasimhalu discloses, "The signature is derived from an arbitrarily selected list of nonuniformities, uniformities and their attributes" (Column 2, lines 20-22) "This signature is used to derive a key for encrypting the information on the storage medium." (Column 2, lines 25-27)

during a write access to the storage device, encrypting data using the cryptographic key and writing the encrypted data to the storage device via the storage drive; and

Narasimhalu discloses, "a key for encrypting the information on the storage medium." – Column 2, lines 25-27)

during a read access to the storage device, reading encrypted data from the storage device and decrypting the data using the cryptographic key.

Narasimhalu discloses, "Decryption of the information is accomplished by generating a key...." (Column 2, lines 39-41)

29. Claim 33 states:

The method of claim 32, wherein the drive-specific information includes a drive serial number.

Narasimhalu discloses, "One such method uses as key the hardware serial number or identification number." (Column 1, lines 37-38)

30. Claim 42 states:

A computer-readable medium having computer-executable instructions for

performing the method of retrieving drive-specific information from a storage drive;

Narasimhalu discloses, "The detailed description with respect to the copy protection scheme using medium signature is presented partially in terms of algorithm and symbolic representation upon operation on data bits within the computer memory." (Column 3, lines 17-20)

"An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. These steps are those require physical manipulation of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, and otherwise manipulated." (Column 3, lines 25-31)

"Electrical or magnetic signals capable of being stored, transferred, combined, and otherwise manipulated" is read to include "a computer-readable medium having computer-executable instructions."

Narasimhalu also discloses "nonuniformities 41-47 are detected with a nonuniformities detection program (NDP)." (Column 4, lines 35-36) "Sensing a storage device" is read to comprise "retrieving drive-specific information from a storage drive."

generating a cryptographic key as a function of the drive-specific information;

Narasimhalu discloses, "The signature is derived from an arbitrarily selected list of nonuniformities, uniformities and their attributes" (Column 2, lines 20-22)

"This signature is used to derive a key for encrypting the information on the storage medium." (Column 2, lines 25-27)

during a write access to the storage device, encrypting data using the cryptographic key and writing the encrypted data to the storage device via the storage drive; and

Narasimhalu discloses, "a key for encrypting the information on the storage medium." – Column 2, lines 25-27) "Encrypting the information on the storage medium" is read to include "writing via the storage drive."

> during a read access to the storage device, reading encrypted data from the storage device and decrypting the data using the cryptographic key.

Narasimhalu discloses, "Decryption of the information is accomplished by generating a key from both the signature of the distribution medium and the DID-S." (Column 2, lines 39-41) "From both the signature of the distribution medium" is read to include "reading encrypted data from the storage device."

31. Claim 43 states:

> The computer-readable medium of claim 42, wherein the drive-specific information includes a drive serial number.

Narasimhalu discloses, "One such method uses as key the hardware serial number or identification number." (Column 1, lines 37-38)

32. Claim 45 states:

> A computer-readable medium having computer-executable instructions for performing the method of sensing whether a storage device has security information stored thereon;

Narasimhalu discloses, "The detailed description with respect to the copy protection scheme using medium signature is presented partially in terms of algorithm and symbolic representation upon operation on data bits within the computer memory." (Column 3, lines 17-20)

"An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. These steps are those require physical manipulation of physical quantities. Usually, though not necessarily, these

quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, and otherwise manipulated." (Column 3, lines 25-31)

"Electrical or magnetic signals capable of being stored, transferred, combined, and otherwise manipulated" is read to include "a computer-readable medium having computer-executable instructions."

> operating the computer in a full-access mode when the storage device has the device-specific security information; and

Narasimhalu discloses, "With the decryption key from 220, the present invention enables the information consumer to decrypt the encrypted information (EDI)" (Column 7, lines 26-29)

> operating the computer in a restricted-access mode when the storage device does not have the device-specific security information.

Narasimhalu discloses, "There are two possibilities for the incorrect signature: (1) a read/write peripheral fails to transfer the nonuniformities from the distribution medium to a copied medium, or (2) the storage medium is a copied or unauthorized medium. Both outcomes are detected by the SVP in step 175. It follows that an evade program is invoked in step 180 to halt the program altogether." (Column 6, line 67 – Column 7, line 6) "To halt the program altogether" is read "to prevent data from being written to the storage device..."

33. Claim 46 states:

> The computer-readable medium of claim 45, wherein operating the computer in a full-access mode includes the following:
> encrypting digital data to be written to the storage disk; and
> decrypting digital data read from the storage device.

Narasimhalu discloses, "a key for encrypting the information on the storage medium." (Column 2, lines 25-27)

Narasimhalu discloses, "Decryption of the information is accomplished by generating a key...." (Column 2, lines 39-41)

34. Claims 47-49 are rejected.

Claim 47 states:

> The computer-readable medium of claim 46, wherein the digital data is encrypted and decrypted using a cryptographic key generated from format information for the storage device.

Claim 48 states:

> The computer-readable medium of claim 46, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information etched into the storage device during manufacturing.

Claim 49 states:

> The computer-readable medium of claim 46, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information specific to a removable media drive used for accessing the storage device.

Narasimhalu discloses, "The signature is derived from an arbitrarily selected list of nonuniformities, uniformities and their attributes." Column 2, lines 20-22. Furthermore, "This signature is used to derive a key for encrypting the information on the storage medium." (Column 2, lines 25-27) "List of nonuniformities, uniformities and their attributes" is read to include "format information for the storage device" and "information etched into the storage device during manufacturing."

Furthermore, "by storage medium, the present invention refers to all types of non-volatile storage medium. Examples of such media include floppy disks, hard disks, optical disks and other non-volatile semiconductor storage devices." (Column 1, lines 25-29) is read to include "information specific to a removable media drive used for accessing the storage device"

35. Claim 51 states:

> A computer comprising:
> a drive for accessing a data storage device having security information stored thereon; and

"By storage medium, the present invention refers to all types of non-volatile storage medium. Examples of such media include floppy disks, hard disks, optical disks and other non-volatile semiconductor storage devices." – (Col. 1, lines 25-29) This is read to include "a drive for accessing a data storage device."

"As such, this signature is unique to a given storage medium in the same way finger prints are unique to a human being." (Abstract) This is read as "data storage device having security information stored thereon"

> a storage manager to selectively configure the computer to operate in a full-access mode of operation or a restricted-access mode of operation as a function of the format information and security information stored on the storage device.

Narasimhalu discloses, "A method and apparatus for utilizing medium nonuniformities to prevent the unauthorized duplication and use of digital information..." The "method and apparatus" are read to comprise the "storage manager."

36. Claim 52 states:

> The computer of claim 51, wherein the storage manager generates a cryptographic key as a function of the security information and decrypts data stored on the storage device using the generated key.

37. Claim 61, 63-66 and 67 are rejected under 35 U.S.C. 102(b) as being

anticipated by Michael Angelo, US Patent Number 5887131.

Claim 61 states:

> A computing system comprising:
> a first storage device having format information stored thereon;
> a second storage device having data stored thereon; and
> a software module executing within the computing system, wherein the software module selectively permits access to the data of the second storage device as a function of the format information and security information stored on the first storage device.

Claim 63 states:

> The computing system of claim 61, wherein the first storage device and second storage device are operatively coupled to a single computer.

Claim 64 states:

> The computing system of claim 61, wherein the software application

generates a cryptographic key as a function of the format information of the first storage device and decrypts the data of the second storage device using the generated key.

Claim 65 states:

The computing system of claim 61, wherein the software application generates a cryptographic key as a function of the format information of the first storage device and format information of the second storage device, and further wherein the software application decrypts the data of the second storage device using the generated key.

Angelo discloses, "the computer checks for the presence of an external token or smart card that is coupled to the computer through specialized hardware. (Col. 3, lines 4-7)(This reads on "a first storage"). The token or smart card is used to store at least one authorization value needed to enable power to the computer system or access to secured resources. (Col2, lines 7-9) (This reads on "format information and security information stored on the first storage device")

Claim 66 states:

A computer comprising:
a storage drive operating in a read-only mode upon power-up,
a storage device operably coupled to the storage drive, wherein the storage device has security information stored thereon; and
a storage manager to selectively configure the storage drive to operate in read/write mode as a function of the security information stored on the storage device.

Angelo discloses, "...hard drives and other storage devices have been created which prevent data access operations on the hard drive upon power-up until the user enters a password. The password is located on the disk itself ..." (Col. 2, lines 54-57)

Claim 67 states:

The computer of claim 66, wherein the software application generates a cryptographic key as a function of the format information, verifies the

> security information on the storage device using the generated key and, upon verification, configures the storage drive to operate in read/write mode.

Angelo discloses, "The token or smart card is used to store at least one authorization value needed to enable power to the computer system or access to secured resources. " (Col. 5, lines 7-9) Furthermore, "once entered, a one-way hash function is performed on the user password. The resulting hash value is compared to an authentication value (token value) downloaded from the token. If the two values match, the power-on sequence is completed and access to the computer system and/or secured computer resources is permitted. If the two values do not match, power to the entire computer system and/or secured computer resources are disabled." (Col. 5, lines 13-18)

38. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

39. Claims 7, 9-11, 20-25, 34-38, 44, 50, 55 and 62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narasimhalu et al. (U.S. Patent Number 5,412,718) in view of Moore (U.S. Patent Number (6,067,622).

Claim 7 states:

> The method of claim 5, wherein the drive-specific information includes calibration parameters for the drive.

Claim 34 states:

The method of claim 32, wherein the drive-specific information includes calibration parameters for the drive.

Claim 35 states:

The method of claim 34, wherein the calibration parameters includes configuration parameters for read and write circuitry internal to the storage device.

Claim 36 states:

The method of claim 35, wherein the calibration parameters are selected from the following set of calibration parameters for the storage drive: tracking parameters, a read channel boost, frequency cutoff values, read threshold values, alignment values, optical alignment correction factors and analog to digital conversion calibrations.

Claim 44 states:

The computer-readable medium of claim 42, wherein the drive-specific information includes calibration parameters for the drive.

Moore discloses "For example, the "internal run key" can be determined by means of an algorithm employing the descriptive number with respect to the processor employed by the computer, the bus size of the computer, the hard disk interleave value, etc." This is read to include all parameters related to the drive calibration information.

While Narasimhalu teaches encryption / access control based on information of the storage device, it does not specifically specifies calibration information which Moore mentions. It would have been

obvious to one of ordinary skill in the art to modify the Narasimhalu invention to include calibration information as input to key generation. The motivation to do so would have been that "Copy protection schemes that incorporate some characteristic in the purchased software package which can be detected by a standard disk drive, but which cannot be reproduced by the drive, have not been found to be very effective as the usual mechanical tolerances found in disk drives minimizes the efficacy of such schemes." (Col. 4, lines 32 – 38)

40. Claims 9 –11, 62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narasimhalu et al. (U.S. Patent Number 5,412,718) in view of Watson et al. (U.S. Patent Number 5,475,839).

Claim 9 states:

> The method of claim 1, wherein operating the computer in a full-access mode includes permitting the user to access sensitive data stored on a remote computer.

Claim 10 states:

> The method of claim 1, wherein operating the computer in a full-access mode includes permitting the user to access a second storage device.

Claim 11 states:

> The method of claim 10, wherein operating the computer in a full-access mode includes decrypting digital data read from a second storage device using a cryptographic key generated from the device-specific security information.

Claim 62 states:

> The computing system of claim 61, wherein the first storage device and second storage device are operatively coupled to two different computers

that are communicatively coupled via a network.

Watson discloses, "a method and structure is taught which allows a supervisor or security officer to control security information stored locally in individual PCs remotely, for example via a host computer on the network to which the PC is connected."

"Control security information stored locally in individual PCs remotely" is read to include "decrypting digital data read from a second storage device." (From claim 10 & 11)

While Narasimhalu discloses enabling security/encryption to the local computer, Watson teaches accessing remote PCs.

It would have been obvious to one of ordinary skill in the art to modify the Narasimhalu invention to extend the access to remote computers. The motivation to do so would have been to allow information to be shared among multiple computers "authorized PC users can legitimately download large amounts of mainframe information." (Watson - Col. 1, lines 28-29)

41. Claim 20 and 21 are reproduced here as references for claims 22-25 which follow:

Claim 20 states:

> A method for accessing a storage device comprising:
> detecting.a storage device within the storage drive;
> sensing whether a storage device has device-specific security information stored thereon;
> encrypting digital data using the device-specific security information when the storage device has the device-specific security information;
> and writing the encrypted digital data to the storage device.

Claim 21 states:

> The method of claim 20, wherein encrypting digital data using the device-specific security information generating a cryptographic key as a function of low-level format information for the storage device.

42. Claim 22-25, 50 rejected under 35 U.S.C. 103(a) as being unpatentable over Narasimhalu et al. (U.S. Patent Number 5,412,718) in view of Epstein (U.S. Patent Application Number 20020124176A1).

Claim 22 states:

> The method of claim 21, wherein encrypting digital data using the device specific security information includes generating a cryptographic key as a function of user-specific security information.

Claim 23 states

> The method of claim 22, wherein the user-specific security information is a password.

Claim 50 states:

> The computer-readable medium of claim 46, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information specific to a user.

Claim 55 states:

> The computer of claim 51, wherein the storage manager generates a cryptographic key as a function of the format information and user-specific information and decrypts data on the storage device using the generated key.

Epstein discloses, "For example, the token may merely contain an encryption of a user's PIN," (Page 4, paragraph 33, line 7). In this instance, "password" is read to include "a user's PIN" and "an encryption of a user's PIN" is read as the PIN being used to generate the cryptographic keys.

"PIN" is read as the user's Personal Identification Number in this example's context where Epstein further discloses "the user to type in the PIN at a conventional ATM machine..." (Page 4, paragraph 33, lines 10-11).

Epstein also precedes this example with, "As presented thus far, the preferred embodiment of the invention includes high-security public/private asymmetric keys and a challenge-response security protocol. As would be evident to one of ordinary skill in the art, less complex methods may be used, albeit with an accompanying decrease in the level of security provided."

This suggests different possible combinations of encryption and security means such as using a password instead of a PIN.

43. Claims 24 & 25 are rejected as follows:

Claim 24 states:

> The method of claim 22, wherein the user-specific security information is biometric information.

Epstein discloses, "Preferably, the biometric information contains a sufficient resolution to generate at least as many bits as the number of bits in the encryption key." (Page 3, paragraph 26, lines 18-20)

Claim 25 states:

> The method of claim 24, wherein the biometic[sic] information is digital output from a retina scanner or a fingerprint scan.

Epstein discloses, "Biometric information, such as fingerprints, retina patterns, voice prints and the like, is often used to uniquely identify individuals." (Page 1, Paragraph 0004, lines 1-3)

While Narasimhalu et al. disclose using « nonuniformities, uniformities and attributes" to generate encryption methods for access control, Davies teaches so using other means such as user-based information like biometrics. It would have been obvious to one of ordinary skill in the art to modify the Narasimhalu invention to accept biometrics as a means of additional security level. The motivation to do so would have been to enhance the security – "more secure, easier to use" (Epstein – Col.1, paragraph 0005, lines 1-6)

Claims 37 & 38 are rejected as follows:

Claim 37 states:

> A method for securely accessing a plurality of storage devices within a storage drive comprising:
> retrieving format information from a first storage device;
> retrieving format information from a second storage device; and
> generating a cryptographic key as a function of the format information for the first storage device and the format information for the second storage device.

Claim 38 states:

> The method of claim 37, and further including:
> encrypting data using the cryptographic key during a write access to either the first storage device or the second storage device; and
> reading encrypted data and decrypting the read data using the cryptographic key during a read access to either the first storage device or the second storage device.

Narasimhalu teaches, "A method and apparatus for utilizing medium nonuniformities to prevent the unauthorized duplication and use of digital information...", "By storage medium, the present invention refers to all types of

non-volatile storage medium. Examples of such media include floppy disks, hard disks, optical disks and other non-volatile semiconductor storage devices. ", and further discloses, "It is contemplated that many changes and modifications may be made by one of ordinary skill in the art without departing from the spirit and the scope of the invention as described." "Floppy disks" comprise of a two-sided storage area (read device). Therefore, it would have been obvious to one skilled in the art to use Narasimhalu's invention for a plurality of storage devices. The motivation to do so would have been to prevent one from bypassing the access control of the PC/network by using a storage device that did not implement Narasimhalu's invention.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurent Trieu whose telephone number is 703-305-0712. The examiner can normally be reached on Monday - Friday, 7AM - 4PM ET.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-746-5447.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

***

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100